CIVO NAVIGATE

Europe 2023

Scratching an Itch

Running Policy in Hard To Reach Places With Wasm & OPA

Charlie Egan - Styra

@charlieegan3 charlieegan3.com/talks/opa-wasm

@CivoCloud

Talking today

Charlie Egan
Developer Advocate @ Styra

https://charlieegan3.com/talks/opa-wasm

Twitter
@charlieegan3

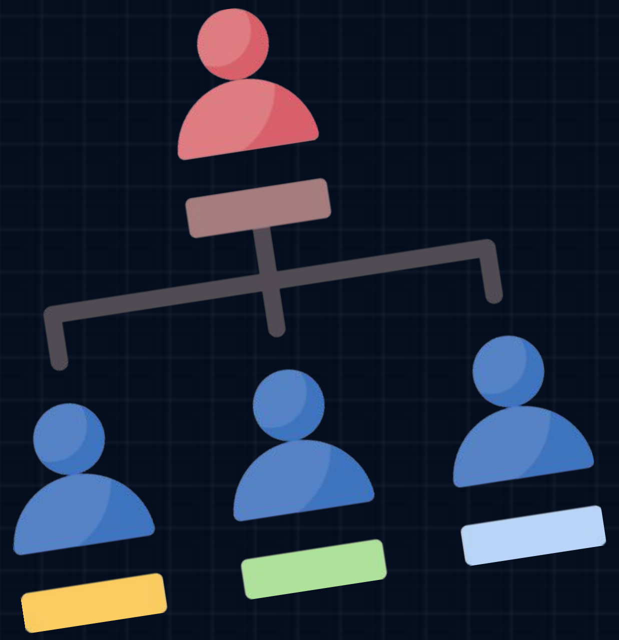
Mastodon
hachyderm.io/@charlieegan3

charlie@styra.com
charlieegan3.com

What are Policies?

(What I mean when I talk about policies)

What are Policies?



“Only admins are allowed”

“Users in the human resources department can update salary information”

images: Freepik on Flaticon.com

What are Policies?

"Customers can't book plane seats in row 13"

images: Freepik on Flaticon.com

What are Policies?

“The product can only be sold between January 1st and the first Sunday after the full Moon that occurs on or after the spring equinox”

What are Policies?

“The product is sold between January 1st and the first Sunday after the full Moon that occurs on or after the spring equinox”

images: Freepik on Flaticon.com

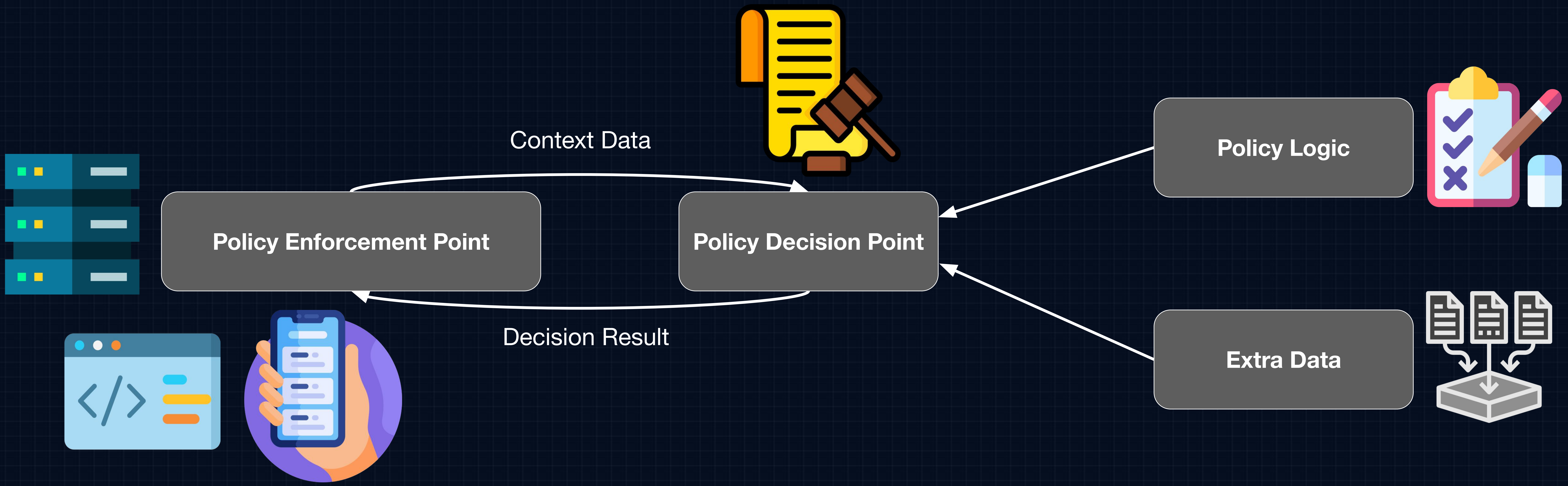
Businesses are built on policies

images: Eucalyp on Flaticon.com

What is Policy Evaluation?

What is Policy Evaluation?

In a generic sense…



Context Data

Policy Enforcement Point

Policy Decision Point

Decision Result

Policy Logic

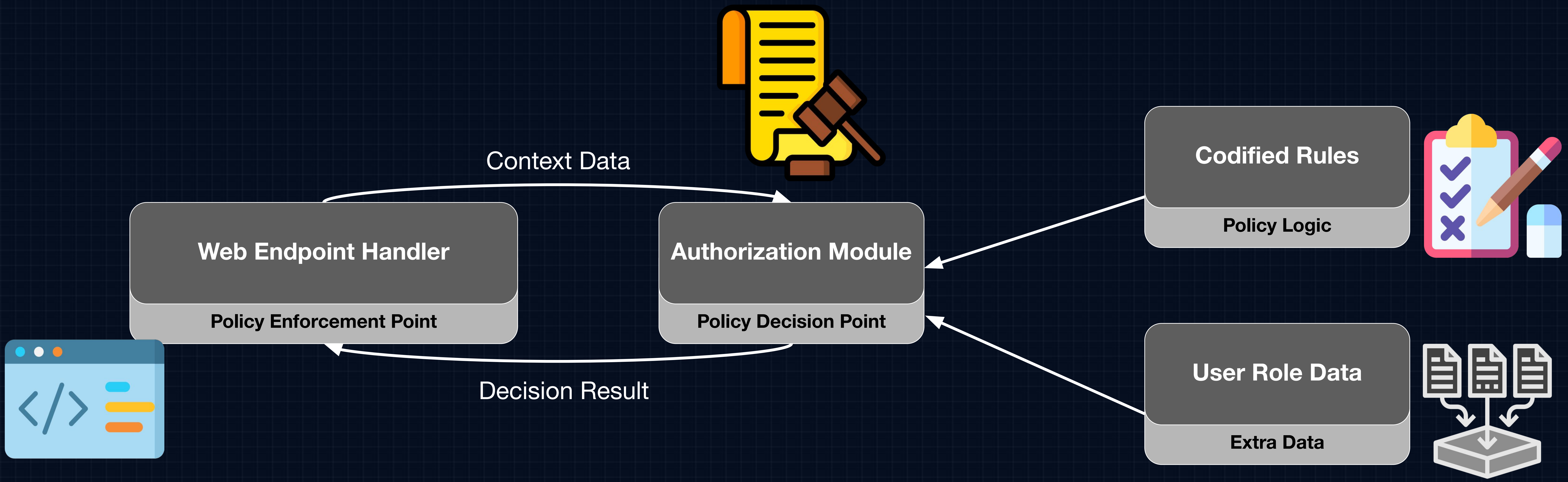
Extra Data

images: Freepik, Karma, Smashicons & Becris on Flaticon.com

What is Policy Evaluation?

CIVO NAVIGATE Europe 2023

Inside a **single application…**

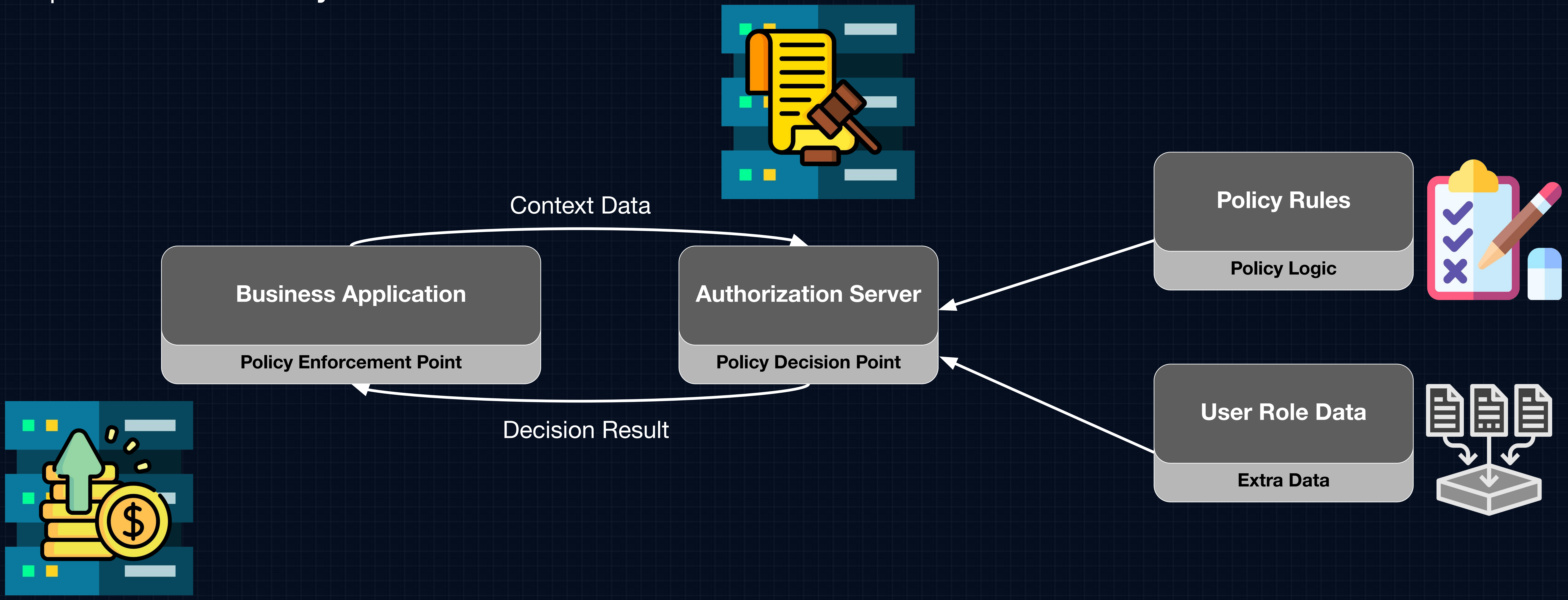


images: Freepik, Karma, Smashicons & Becris on Flaticon.com

@CivoCloud

What is Policy Evaluation?

As part of a **distributed system…**

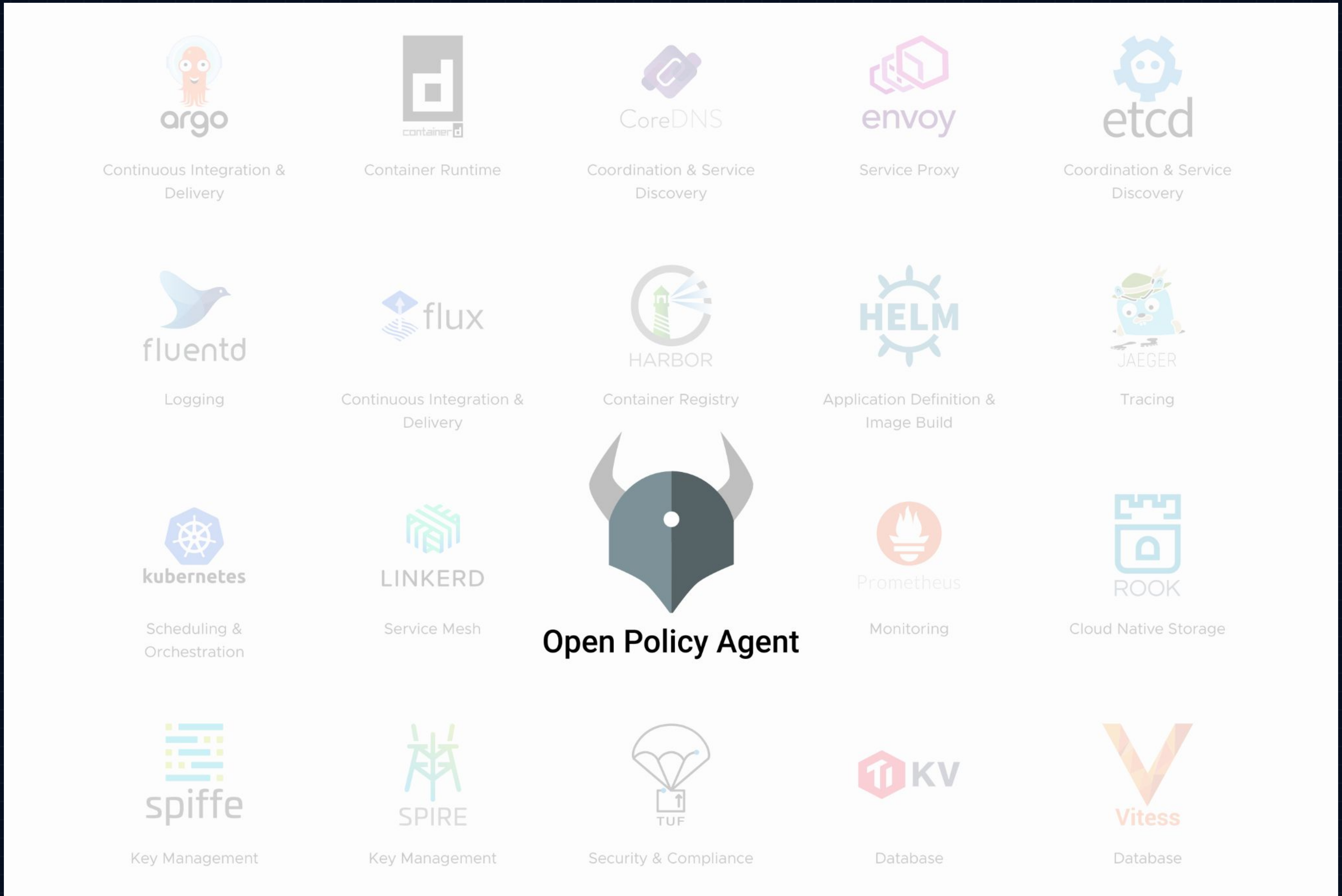


images: Freepik, Karma, Smashicons & Becris on Flaticon.com

Open Policy Agent?

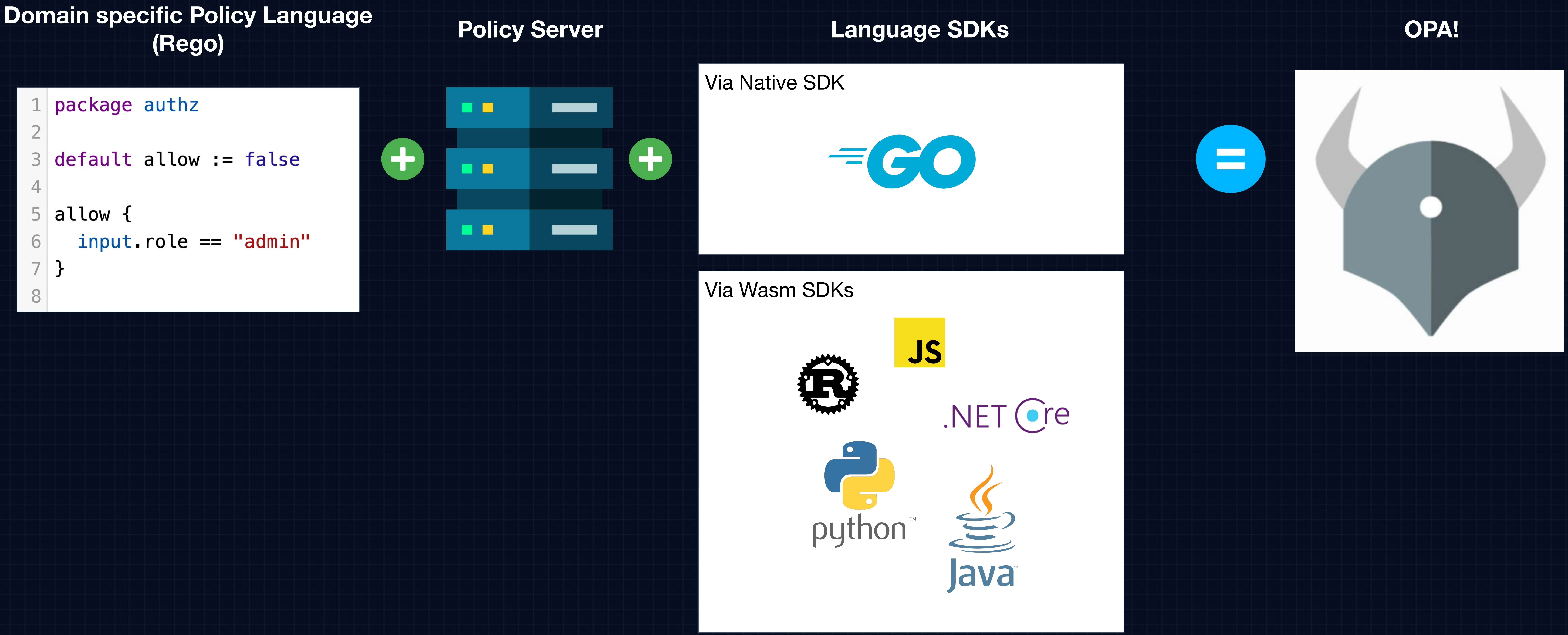
images: Eucalyp on Flaticon.com

Open Policy Agent: Intro



CIVO NAVIGATE Europe 2023

Open Policy Agent: Intro



Domain specific Policy Language (Rego)

```
package authz

default allow := false

allow {
  input.role == "admin"
}

```

Policy Server

Language SDKs

Via Native SDK

Via Wasm SDKs

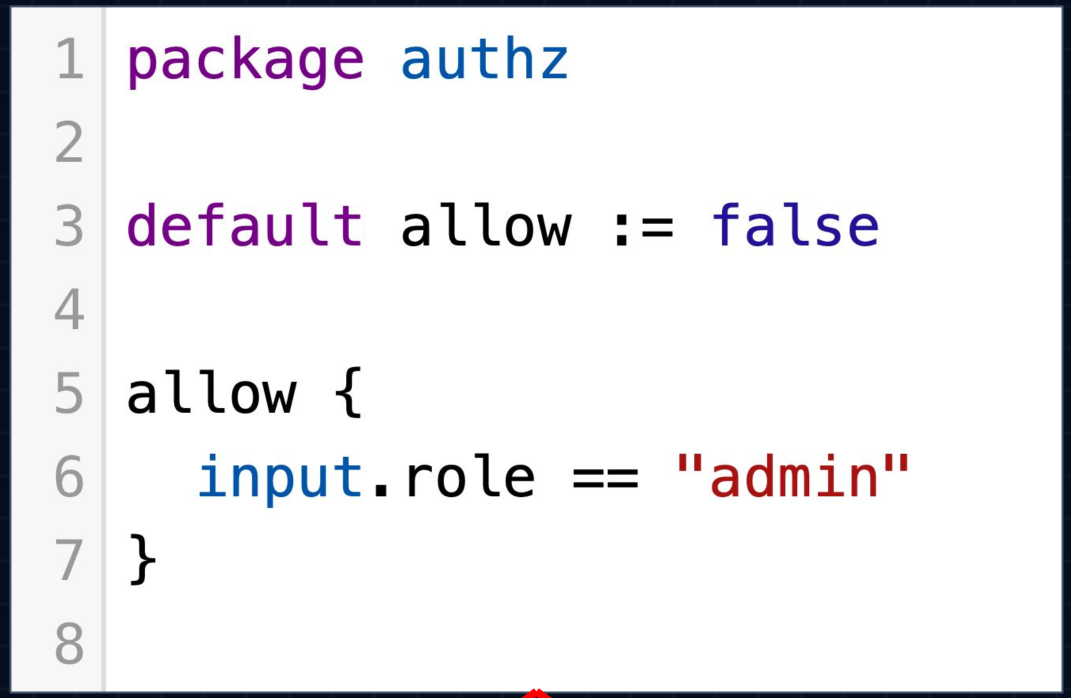
OPA!

icons: Freepik, kliwir art on Flaticon

@CivoCloud

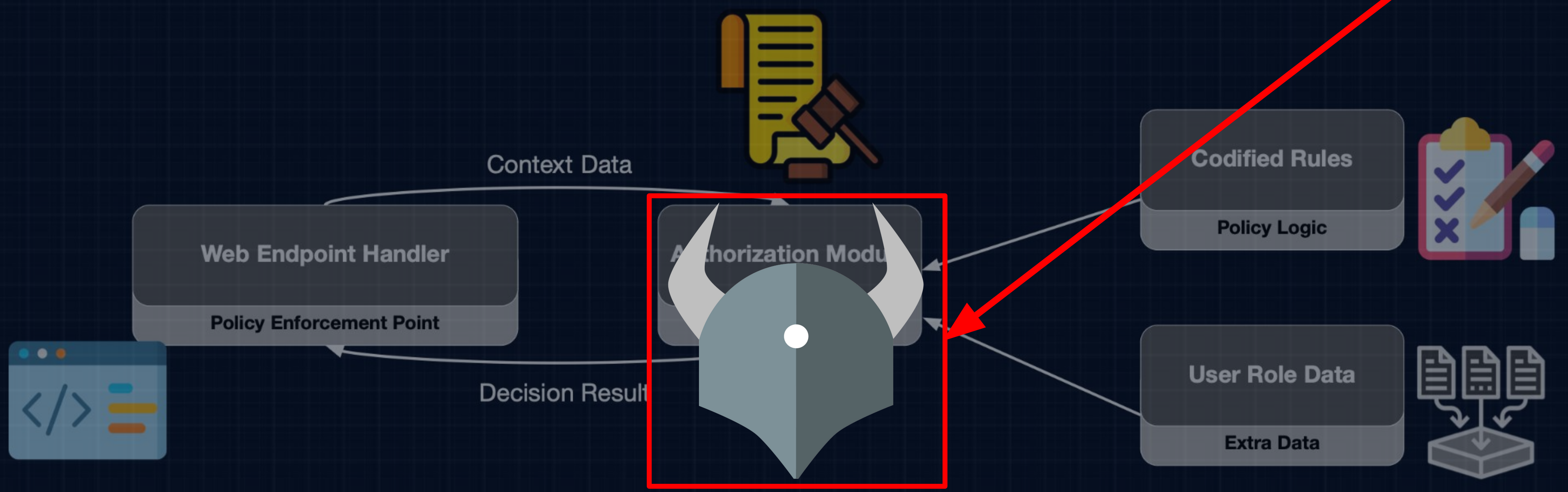
Open Policy Agent: Rego

Rego

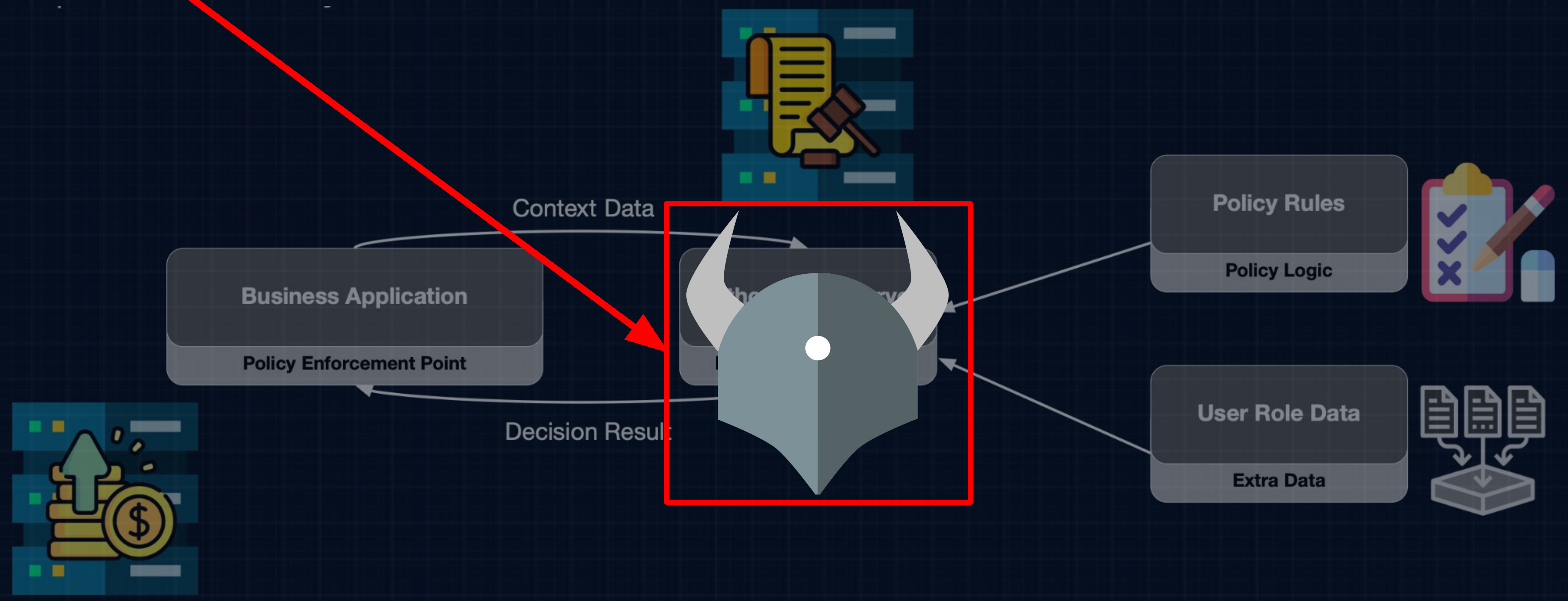


```
package authz

default allow := false

allow {
  input.role == "admin"
}

```

Embedded

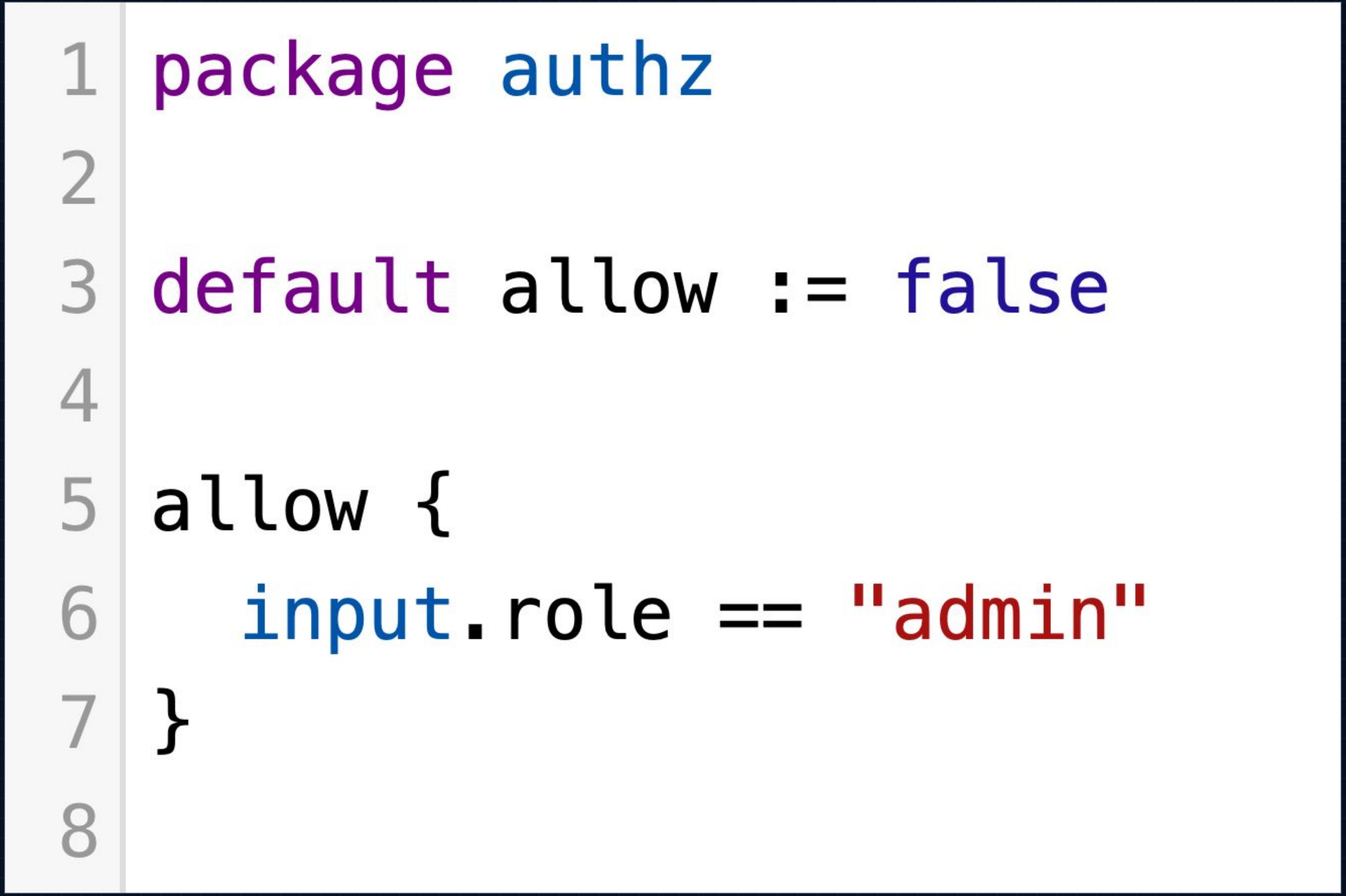


Distributed / Server invoked

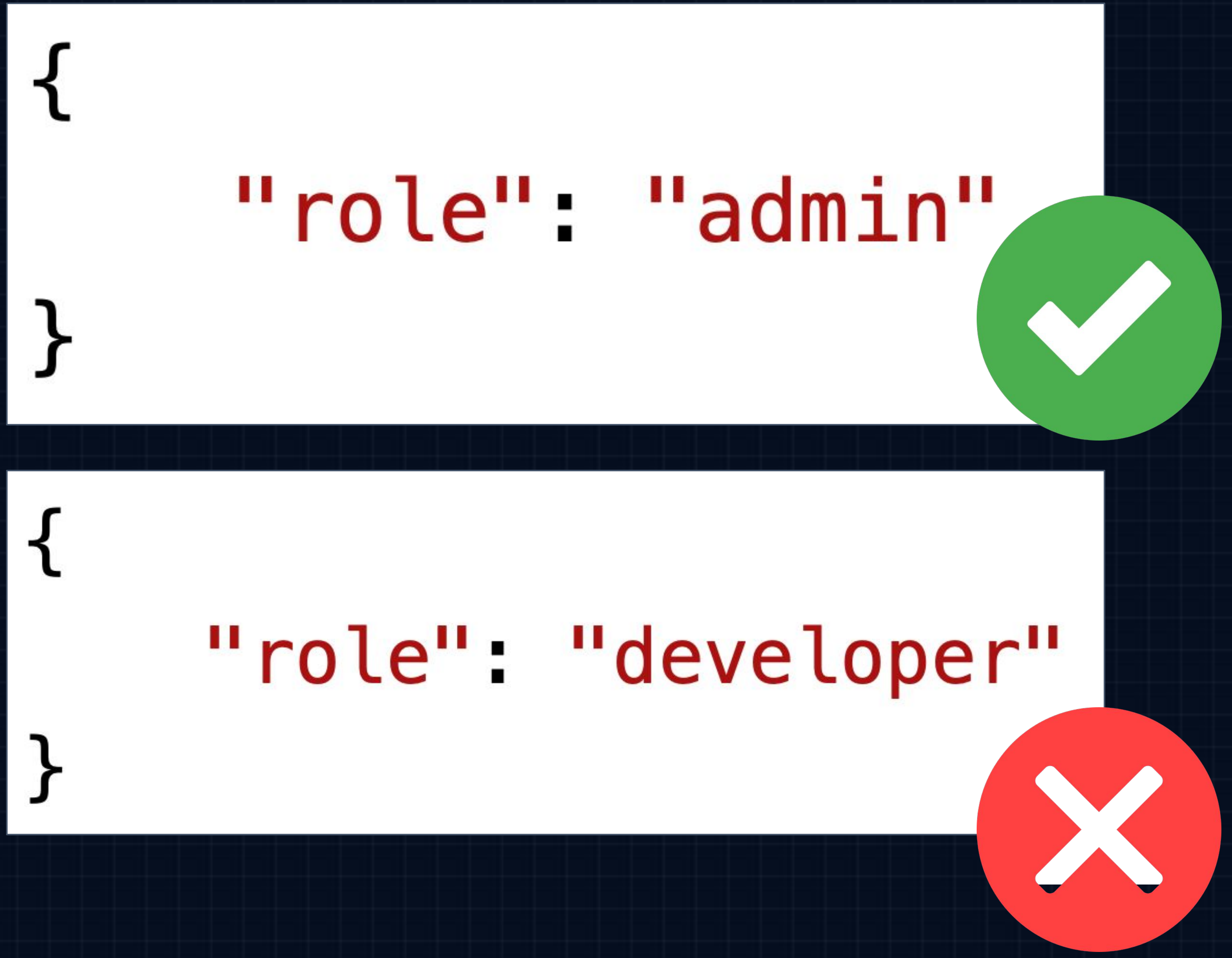


images: Freepik, Karma, Smashicons & Becris on Flaticon.com

Open Policy Agent: Rego



```
package authz

default allow := false

allow {
    input.role == "admin"
}

```



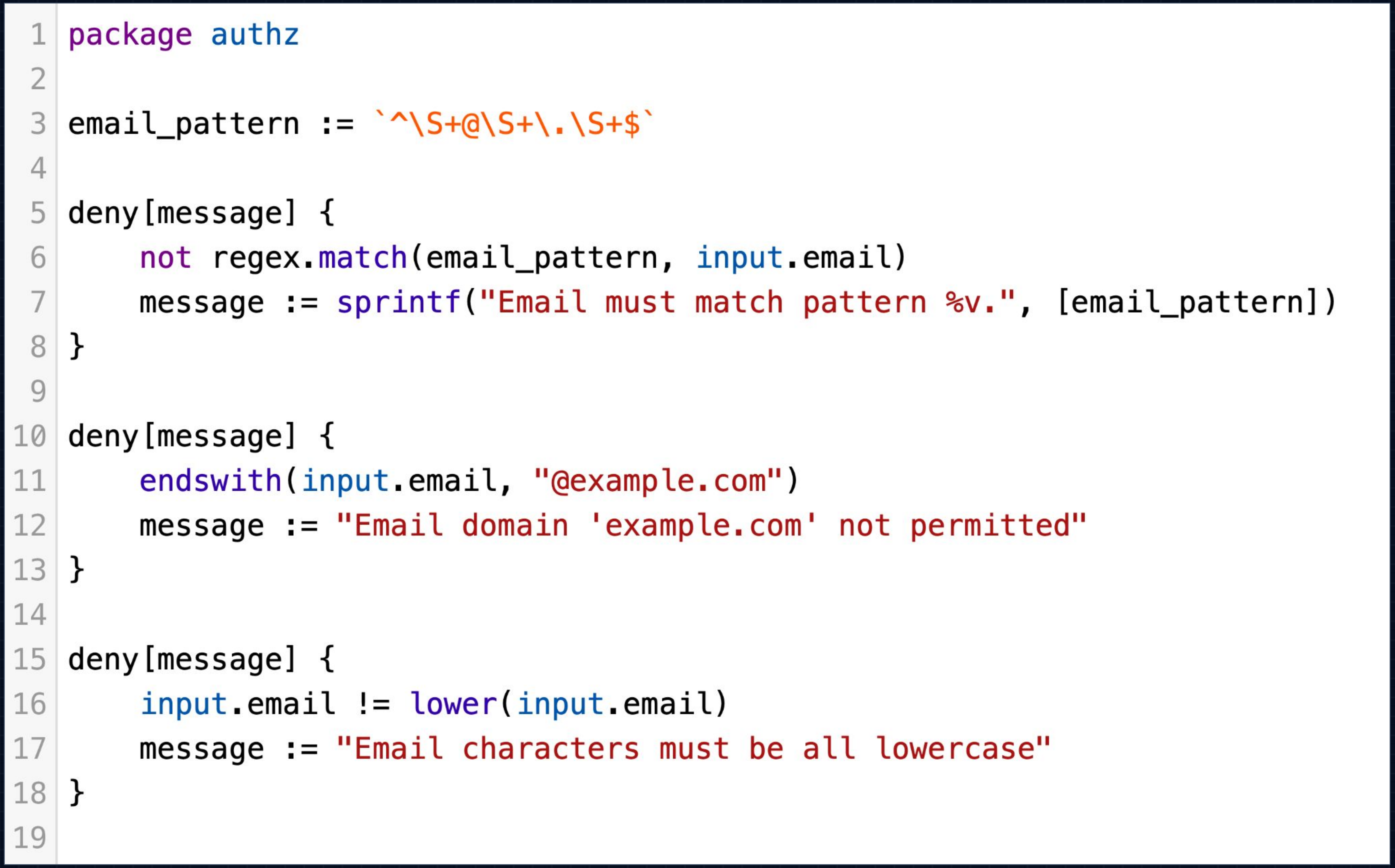
```
{
    "role": "admin"
}
```

✓

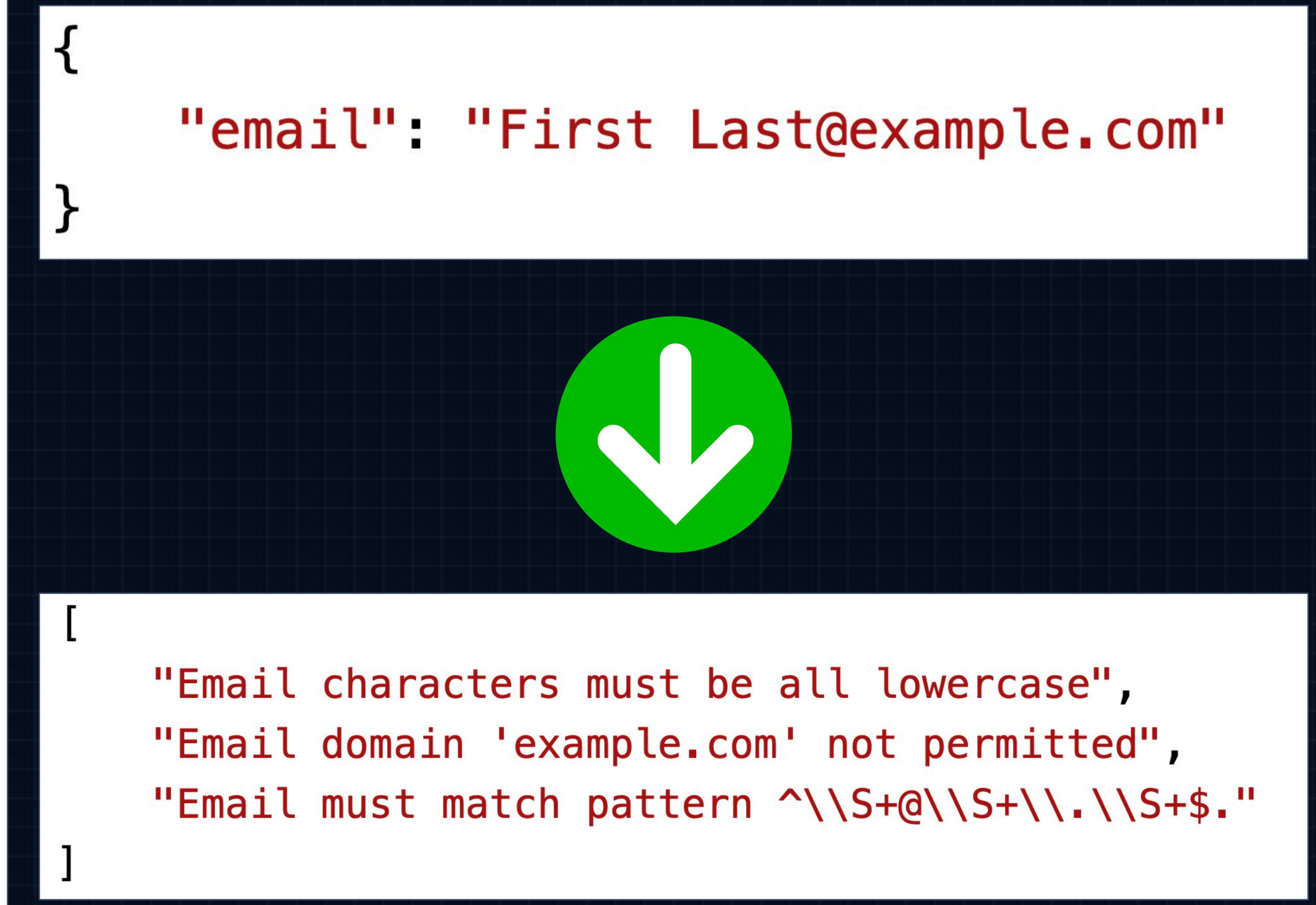
```
{
    "role": "developer"
}
```

✗

Open Policy Agent: Rego



```
package authz

email_pattern := `^\S+@\S+\.\S+$`

deny[message] {
    not regex.match(email_pattern, input.email)
    message := sprintf("Email must match pattern %v.", [email_pattern])
}

deny[message] {
    endswith(input.email, "@example.com")
    message := "Email domain 'example.com' not permitted"
}

deny[message] {
    input.email != lower(input.email)
    message := "Email characters must be all lowercase"
}
```



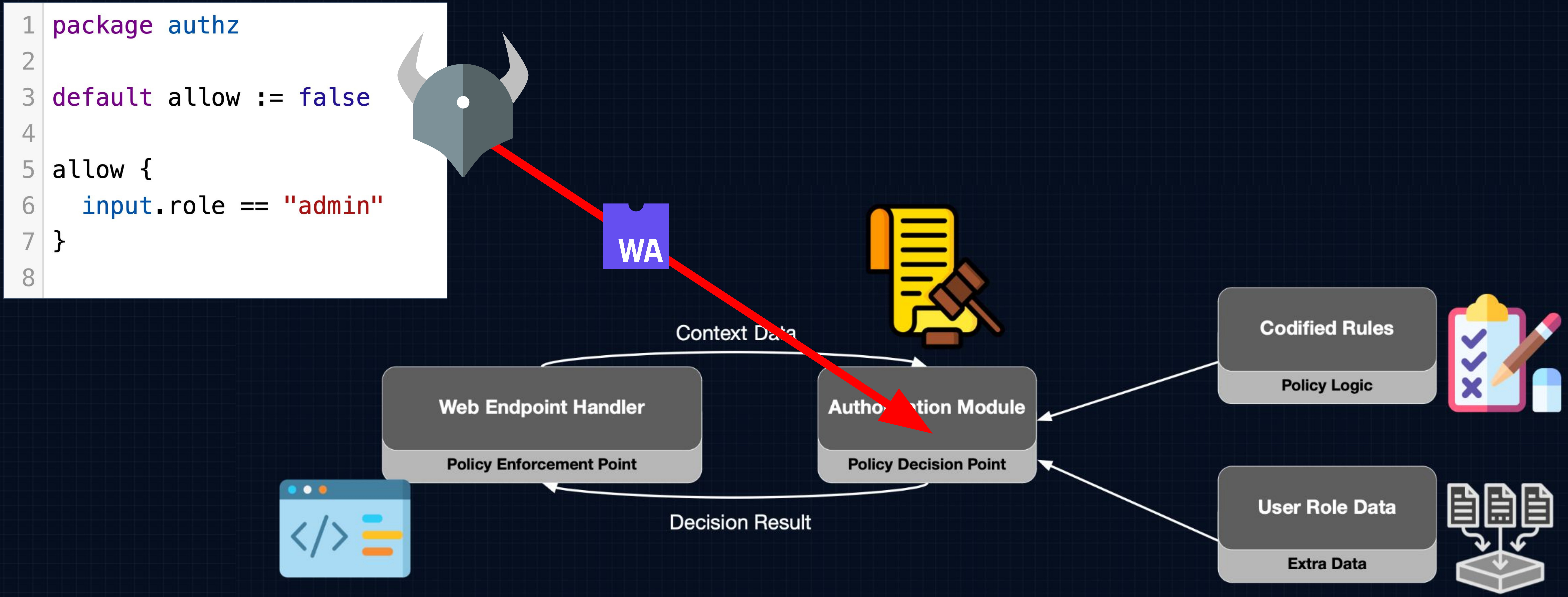
```
{
    "email": "First Last@example.com"
}
```

```
[
    "Email characters must be all lowercase",
    "Email domain 'example.com' not permitted",
    "Email must match pattern ^\\S+@\\S+\\.\\S+$."
]
```

Open Policy Agent: Rego

https://play.openpolicyagent.org/p/VIDtOzzxX8

Open Policy Agent: Wasm



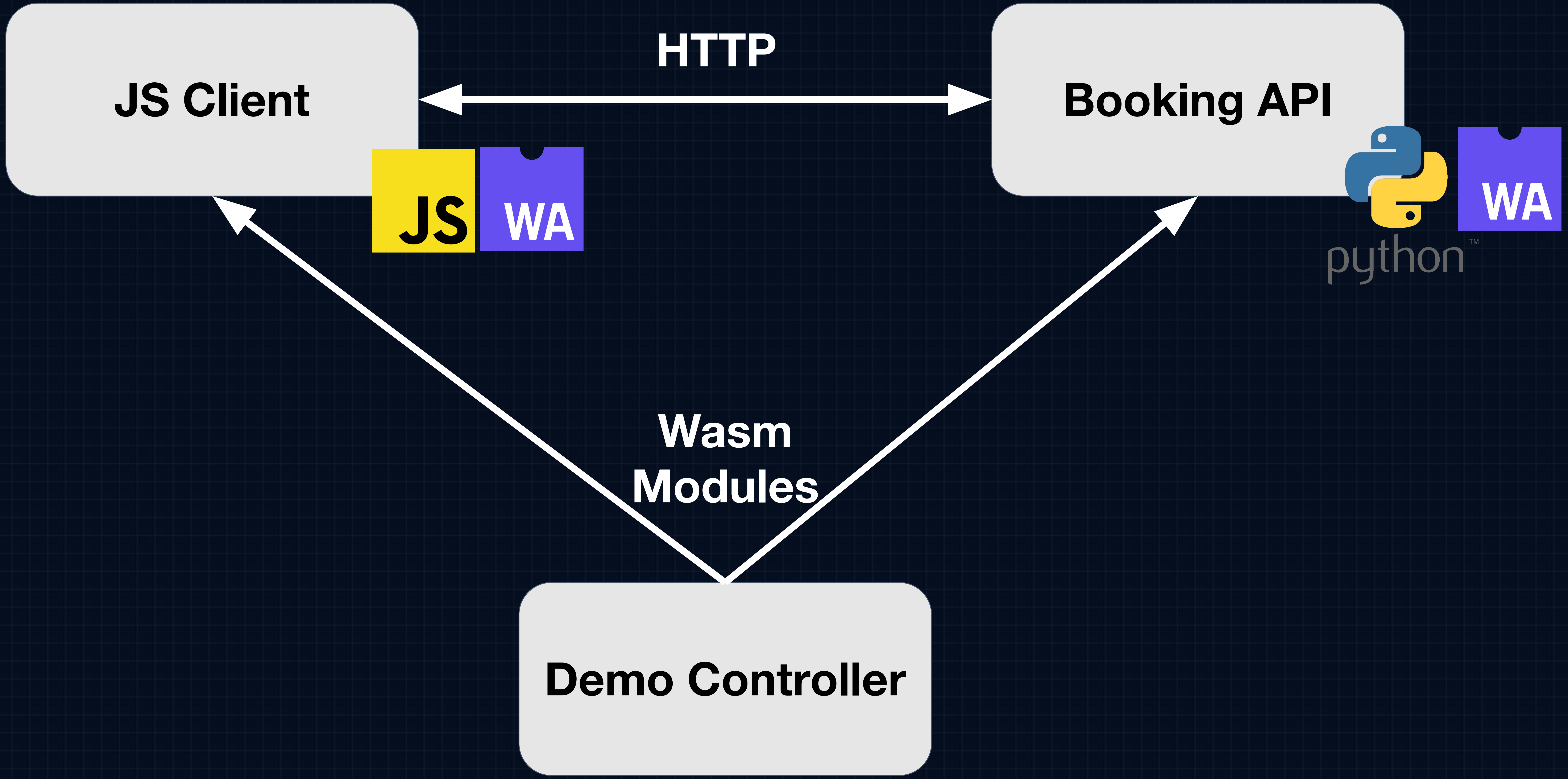
```
package authz

default allow := false

allow {
  input.role == "admin"
}
```

images: Freepik, Karma, Smashicons & Becris on Flaticon.com

Open Policy Agent: Wasm

- Fast feedback to users from client side validation
- Standardised validation logic across suite of related applications
  - Web, mobile, server + other OPA deployments
  - Run OPA in more places
- Improved performance for data intensive policies

Demo


JS Client
JS
WA
HTTP
Booking API
python™
WA
Wasm
Modules
Demo Controller

Wasm in OPA

Past, Present, Future

Wasm in OPA: Past

- 2018: Proof of concept
  - In response to challenges for some users in running a sidecar server
  - & adoption seen elsewhere (Envoy & CDNs like Cloudflare and Fastly)

- Proof of concept showed good performance improvements too
  - https://blog.openpolicyagent.org/opa-v0-15-1-rego-on-webassembly-81c226c51be4

- First official SDK was developed for Node
  - Targeting the Edge/CDN use case

Wasm in OPA: Present

- Good support for building, distributing and evaluating Wasm policy bundles

- Official and community OPA Wasm SDKs for:
  - **Node JS**
  - .NET Core
  - **Python**
  - JVM
  - Rust

- Native Wasm Support for around 50% of Rego built-in functions
  - (Remainder are SDK dependent)

Wasm in OPA: Future

- Candidates for further development (not on roadmap - yet!)
  - Investigate options for data sharing between Wasm threads
    - https://github.com/open-policy-agent/opa/issues/3178
  - Investigate integration with envoy-wasm filters
    - https://github.com/open-policy-agent/opa/issues/3235
  - Support OPA plugins implemented as Wasm modules
    - https://github.com/open-policy-agent/opa/issues/3631
  - Implementation of additional built-in functions in Rego or Language SDKs

(Interest from new contributors in this area would be very welcome :)

Further Reading

All the links, slides etc.
https://charlieegan3.com/talks/opa-wasm

OPA Wasm Docs
https://www.openpolicyagent.org/docs/latest/wasm/

‘Awesome OPA’ Wasm Items (including SDK links)
https://github.com/anderseknert/awesome-opa#webassembly-wasm

OPA PoC Blog (2019)
https://blog.openpolicyagent.org/opa-v0-15-1-rego-on-webassembly-81c226c51be4